Identity Authentication Changeover

Jonathan H. Stechmann[1]

[1] Author has twenty years of experience in product development and large scale identity programs including Photo-IDs, Smartcards and Biometrics; Managed the team that developed and operated the large smart card management system for the American Express Blue Smartcard program; Currently a J.D Candidate, William Mitchell College of Law, 2007; M.B.A., Finance, University of Minnesota Carlson School of Management, 1992; B.S., Computer Science, University of Wisconsin-La Crosse, 1986.

I. INTRODUCTION

As of September 2006, there were over a billion Internet users worldwide.[2] In this age of on-line transactions, personal identification credentials, such as our Social Security Number, ("SSN") are some of our most powerful and treasured possessions. In many instances, such as in government and workplace transactions, we are required to use these identification credentials, but more frequently we are choosing to use these same credentials for discretionary on-line services such as shopping. Identity credentials empower on-line efficiency, thus creating time to spend with family and friends.

The growing problem of identity theft is well documented, but the consequences of being one of the unfortunate victims of identity theft are under appreciated. Estimates are that 25% of adults have been affected by identity theft. Annual financial losses from identity theft have been estimated to cost Americans fifty-three billion dollars.[3] More shocking is the estimate that

---

[2] *See* http://www.internetworldstats.com/stats.htm (Internet-world-stats, Internet Usage Statistics: The Big Picture, 1,086,250,903 users last updated Sept. 18, 2006).

[3] Department of Justice, FBI, *Financial Crimes Report to the Public*, May 2005.

20% of identity theft victims do not even find out they are victims until two years after the theft.[4]

The use of a common identifier, namely an individual's SSN, as the main authentication element is one of the major factors creating the identity theft problem. The second major factor is the failure to properly safeguard these identity credentials. The Privacy Act of 1974 ("the "Privacy Act") provides a remedy for individuals to bring civil actions against the government for violations concerning the individual's personal information.

The Supreme Court's decision in *Doe v. Chao*[5] represented a major setback in the ability of individuals to recover damages under the Privacy Act. The Court held that the government's "intentional and willful" disclosure of the plaintiff's SSN represented an adverse effect to the victim, and constituted a violation of the Privacy Act, but without proof of "actual damages" the victim could not receive compensation. The issue the Court chose to address is whether a plaintiff must prove actual damages to recover the minimal statutory award of $1,000. The Court's holding that no actual damages equals no recovery,

[4] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1248 (2003).

[5] 540 U.S. 614 (2004).

for all practical purposes, places zero value on the disclosure of a SSN, our most treasured identity credential.[6]

A major change is required in how lawmakers and the courts value disclosed identification credentials. Courts should impose a higher standard for both government and private enterprises (collectively "Enterprises") in safeguarding personal identification credentials. The famous *T.J. Hooper* case is used to illustrate the point that proven technology exists to fix this identity authentication problem, and Enterprises should not be allowed to use the shield of custom to justify negligent identity management.[7] Unfortunately, the Supreme Court's holding in *Doe v. Chao* has done nothing to deter identity theft by placing zero value on the loss of identification credentials.

If Enterprises were held liable for a realistic value associated with the loss of identity credentials and if Enterprises were not allowed to rely on the industry's outdated identity management customs as a defense, then, the free market would quickly resolve the current identity authentication problem with a new model. Such model would require Enterprises to use an identifier other than the SSN for primary

---

[6] *Id.*

[7] T.J. Hooper, 60 F.2d 737 (1932).

authentication and would deploy strong authentication technologies based on cryptography and biometrics for on-line transactions.

II. ANALYSIS

A. No Justice for Identity Theft Victims

The Supreme Court's stingy interpretation of the Privacy Act's damages provision will result in fewer individuals willing to invest the time and effort to hold Enterprises accountable for not properly safeguarding identity credentials. The Supreme Court missed a great opportunity hold Enterprises accountable for the loss of valuable identity credentials. The Court chose to engage in a technical debate over the textual structure of the Privacy Act's damages provision, verses taking on the real issues of how to place a value on the loss of identity credentials in the Internet era.

B. Attacking Identity Theft through the Legislature and the Courts.

The identity theft problem has reached the point where something significant needs to be done. Identity theft threatens our national economy, national security, trust in free enterprise, and trust in our government. The three branches of government must work with the private sector to attack identity theft. It is my opinion that identity theft can not be controlled or fixed without changing how we authenticate individuals in the current age of on-line everything.

Ultimately private Enterprises need to implement this new identity authentication platform, but Congress and the courts play the critical role of initiating this change by imposing liability and painful damages for disclosure of identity credentials.

1. Citizen Action

Most importantly, citizens must really want to fix this problem and must be willing to make some short-term sacrifices to get there. The explosion of new identity theft legislation and the President's Executive Order creating an Identity Theft Task Force should indicate the priority and the amount of money being spent on this problem.

Taxpaying citizens have a vested interest in fixing this problem in the most efficient way possible. Two old adages come to mind: first, "Don't throw good money after bad"; and second, "You can pay me now or pay me later." In my opinion, there is not enough money in the world to police, prosecute, and punish identity theft without fundamentally changing our authentication model. Significant taxpayer dollars may be able to contain the problem for a couple years, but expensive policing will not benefit the long-term fix. I propose that the most efficient way to solve this problem is to start today by supporting Congress in enacting laws that impose negligence standards and liability for mere disclosure of identity credentials.

2. Legislative Action

Congress plays a key role in setting the tone and shaping our national identity protection policy. The breadth of identity theft risk has been exponentially enabled by Internet technologies. Identity theft today is primarily a technology crime. Ultimately, the problem can only be solved by using more sophisticated technology. Cynics would argue that deployable technology for strong authentication has been around for many years, and that if this technology could really solve the problem, it would have been implemented by now. This argument would be credible if the free enterprise system was allowed to work freely. However, laws and weak enforcement have artificially protected Enterprises from liability. Enterprises have relied on pro-business laws and the shield of custom to justify keeping outdated identity authentication techniques.

There are several actions Congress can take to initiate our national identity authentication changeover. First, Congress should clarify the wording in the damages section of the Privacy Act to ensure liquidated damages are paid regardless of proof of actual damages. Second, Congress should increase the amount of liquidated damages from $1000 to $5000. These two changes taken together will basically place a monetary value on the mere disclosure of an individual’s identity credentials. Also, any disclosure of identity credentials represents an adverse effect.

While this is a harsh monetary penalty for the disclosing Enterprise, the intent of the policy is to get Enterprises to stop using SSNs and to use extreme care in safeguarding other identity credentials. Third, Congress should ensure that citizen enforcement remedies are included in all identity theft prevention legislation. Civil remedies are the most effective way to hold Enterprises accountable. Finally, Congress should adopt an across-the-board negligence standard for safeguarding of identity credentials.

a. Negligence Standard

While recent identity theft legislation focused on the thieves is welcomed, it makes little impact on solving the problem. In order to truly address this problem, legislation needs to go where the money is and impose simple negligence standards and liability on Enterprises entrusted with holding identity credentials. The courts will be asked to hold Enterprises to a reasonable standard of care.

3. Judicial Action

The Judicial branch must play a decisive role in our national identity protection policy. There are three areas that require thoughtful court participation.

First, the courts must enforce the privacy laws enacted by Congress and embrace the policy of valuing identity credentials. The court should not be afraid to impose painful monetary

damages on Enterprises for disclosure of identity credentials. The court must understand that the penalties are important to force Enterprises the change the way they do business. The courts should be reminded that fears of enormous costs from enforcement of the Privacy Act, never materialized.[8] Before the Privacy Act passed, the OMB estimated a total of $300-$400 million to implement the Privacy Act in 1974. The actual cost of implementation in the first year proved to be substantially less - approximately $66 million.

Second, the court must understand the value of identity credential in this on-line world. Bill Gates has said, "The Internet changes everything." With over one billion Internet users[9] a disclosure to any unknown entity must be presumed to be shared with everyone. Relating this new era concept to the Supreme Court's holding in *Doe v. Chao*, the traditional definition of "actual damages" and "adverse effect" come into question. The traditional meaning of actual damages is founded in a physical world and carries the concept of something

---

[8] *Doe*, 540 U.S. at 627-28 (2004) (Ginsburg, J., dissenting) (pointing out that courts have not allowed class certification and runaway liability and that government has not experienced enormous recoveries).

[9] *See supra* note 1.

physical. Does this narrow definition still make sense in this virtual world? The legal definition of actual damages is "an amount awarded to a complainant to compensate for a proven injury or loss; damages that repay actual losses."[10] Could anyone legitimately argue that disclosure of valuable identity credentials is not a proven loss? Or that disclosure of anyone's identity credentials is not an adverse effect? Would the Supreme Court Justices agree with Bill Gates? With a different appreciation for the virtual world, the Supreme Court could have easily found actual damages present for Mr. Doe.

Finally, the Supreme Court is in the powerful and unique position to "in the end say what is required".[11] If Congress does its job and provides identity protection laws containing a liability standard based on negligence, the Supreme Court will have the opportunity to force Enterprises out from behind the shield of custom. The only way for Enterprises to avoid being liable for disclosures would be to utilized advanced strong identity authentication solutions. In my opinion, court imposed liability based on simple negligence is the single most critical step to solving the identity theft crisis.

---

[10] BLACK'S LAW DICTIONARY (8th ed. 2004), damages.

[11] *Hooper*, 60 F.2d at 740.

III. Identity Management Technology

A. Identity Authentication Today

Technology is available to help solve this great societal problem. But, only if the true costs of this problem are exposed will the market feel compelled to implement the technology. While advanced authentication technology has been available for several years, the day-to-day methods of identity authentication have not changed much in generations. Authentication for transactions in the pre-Internet era were based on face-to-face interactions and supplemented with identifying credentials such as name, address, telephone number, driver's license number and SSN. Today, we are still using the same old bundle of identity credentials, but we are conducting more transactions in non-face-to-face sessions.

As transactional technology has evolved, we have taken a step backwards regarding authentication. Today, with on-line transactions we normally just use something we know, our bundle of identity credentials. And the personal identity credentials used are just for enrollment, after enrollment we use an alias username and passwords for subsequent transactions. It is no wonder why identity theft is growing; it is so easy to act as someone else on the Internet. All of us have probably been asked by friends or family to impersonate someone else on the Internet for convenience sake.

B. Why Authentication Must Change in an On-line World

The more factors used in authentication, the better the likelihood of authenticating the correct person. As was described above, our desire to transact on-line has resulted in compromising authentication to the single factor of something we know. Three factor authentication, including something we know, something we have and something we are, is the ideal method for authentication concerning secure on-line transactions.[12]

IV. Scenario for Strong Authentication

The scenario for implementing strong authentication could go something like this. In the not too distant future, the Supreme Court grants certiorari on a case involving disclosure of an individual's identity credentials (SSN, DL, and DOB). The disclosure of the identity information resulted from a computer hacker breaching the system, and was not intentionally disclosed by the Enterprise. The case has no evidence suggesting that any identity thief has used this identity information, but the potential identity theft victim is very concerned by the threat of being economically damaged in the future. The potential victim is outraged by the Enterprise's lack of concern.

[12] This could be accomplished by using a token such as a smart card in combination with a pin and a biometric reader.

The Supreme Court first holds that the baseline value of this individual's disclosed identity information, prior to any proven identity theft is $5,000. The Court arrives at this value by taking into consideration the hours spent by individuals to check, protect and defend their credit records. The presumption is that at some point identity theft will occur as a result of this disclosed information. The Court goes further, holding that this Enterprise, entrusted with this individual's identity credentials, is negligent and liable for not utilizing readily available technology to safeguard this information. The Court's opinion, borrowing from Justice Hand's *T.J. Hooper* holding, may sound something like this.[13]

> The winds of identity theft began to freshen several years ago and Enterprises have had much time to prepare. An identity theft gale is not unusual in this age of on-line transactions; Enterprises entrusted to hold identity information must be ready to meet one. We understand that it is not common practice for Enterprises holding identity credentials to use strong authentication methods. Is it then a final answer that the industry had not yet generally adopted strong authentication? No. "Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[14] But, adequate authentication methods capable of preventing identity theft are readily available at a small cost and are reasonably reliable. And without strong authentication the Enterprises were not trustworthy. The injury to the victim's identity credentials was a direct consequence of the Enterprise's

[13] *Hooper*, 60 F.2d 737.

[14] *Id*.

untrustworthiness, and therefore the Enterprise is liable for damages.

The Court's holding results in millions of dollars paid to potential victims of this isolated disclosure. More importantly, the holding places a monetary value on the loss of each individual's identity credentials and signals that Enterprises cannot use the shield of custom to justify outdated methods for the protection of identity credentials.

Threatened with liability, Enterprises quickly modify their business practices and avoid requesting or holding individual's identity credentials. Enterprises that have a bona fide need for holding identity credentials immediately begin to deploy strong authentication solutions based on public key cryptography and biometrics.

The final step in this identity authentication changeover comes quickly. Private enterprises, burdened with the costs of identity proofing and cross-certification, put pressure on the Federal government to lead the identity authentication initiative and act as the root Certificate Authority. A public/private partnership quickly evolves for the issuance of National Identification smart cards containing unique Private keys and Internet based Public key certificates for every human being living in and transacting with the United States.

V. CONCLUSION

Consumer confidence and trust in the American economy is being seriously threatened by identity theft and Enterprises' inadequate protection of personal identity credentials. Identity authentication technology exists to solve this national problem. While the value and importance of identity credentials used to authenticate individuals for on-line transactions have continued to grow, federal law has failed to recognize this increased value. In fact, not only has the 2004 Supreme Court's decision in *Doe v. Chao* removed incentives for individuals to bring civil enforcement claims against the government under the Privacy Act, but the holding has belittled the value of identity information to zero.[15]

Based on the economic impact resulting from the disclosure of identity information, the Court should first assign a realistic value to the loss of personal identity information, which fairly compensates individuals for the harm. Second, the Court should apply the same strong adjudication as was seen in *T.J. Hooper*,[16] raising the bar on Enterprises entrusted to adequately protect this precious cargo.

---

[15] *Doe*, 540 U.S. at 614.

[16] *Hooper*, 60 F.2d 737.

Faced with liability, threat of serious damages, and no longer shielded from outdated industry custom, Enterprises entrusted with identity credentials will quickly abandon the use of the SSN and adopt strong authentication for on-line transactions.